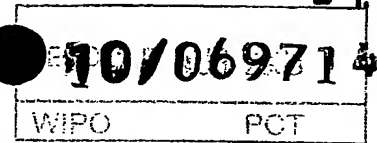




IB 00 / 01157



SCHWEIZERISCHE EIDGENOSSENSCHAFT
CONFÉDÉRATION SUISSE
CONFEDERAZIONE SVIZZERA

Bescheinigung

Die beiliegenden Akten stimmen mit den ursprünglichen technischen Unterlagen des auf der nächsten Seite bezeichneten Patentgesuches für die Schweiz und Liechtenstein überein. Die Schweiz und das Fürstentum Liechtenstein bilden ein einheitliches Schutzgebiet. Der Schutz kann deshalb nur für beide Länder gemeinsam beantragt werden.

Attestation

Les documents ci-joints sont conformes aux pièces techniques originales de la demande de brevet pour la Suisse et le Liechtenstein spécifiée à la page suivante. La Suisse et la Principauté de Liechtenstein constituent un territoire unitaire de protection. La protection ne peut donc être revendiquée que pour l'ensemble des deux Etats.

Attestazione

Gli uniti documenti sono conformi agli atti tecnici originali della domanda di brevetto per la Svizzera e il Liechtenstein specificata nella pagina seguente. La Svizzera e il Principato di Liechtenstein formano un unico territorio di protezione. La protezione può dunque essere rivendicata solamente per l'insieme dei due Stati.

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

Bern, 10. Juli 2000

Eidgenössisches Institut für Geistiges Eigentum
Institut Fédéral de la Propriété Intellectuelle
Istituto Federale della Proprietà Intellettuale

Patentverfahren
Administration des brevets
Amministrazione dei brevetti

Rolf Hofstetter

Best Available Copy

Demande de brevet no 1999 1573/99

CERTIFICAT DE DEPOT (art. 46 al. 5 OBI)

L'Institut Fédéral de la Propriété Intellectuelle accuse réception de la demande de brevet Suisse dont le détail figure ci-dessous.

Titre:
Méthode d'encryptage multi-modules.

Requérant:
NagraCard S.A.
22, route de Genève
1033 Cheseaux-sur-Lausanne

Mandataire:
Griffes Consulting S.A.
81, route de Florissant
1206 Genève

Date du dépôt: 30.08.1999

Classement provisoire: H03M

METHODE D'ENCRYPTAGE MULTI-MODULES

La présente invention concerne le domaine du chiffrement, ou encryptage, et du déchiffrement ou décryptage de données, et particulièrement de données devant rester inaccessibles aux personnes ou appareils non autorisés dans le cadre de systèmes de télévision à péage. Dans de tels systèmes, les données sont chiffrées dans un environnement sécurisé, abritant des puissances de calcul importantes, et appelé sous-système d'encodage, puis envoyées, par des moyens connus en soi, vers au moins un sous-système décentralisé où elles sont déchiffrées, généralement au moyen d'un IRD (Integrated Receiver Decoder) et avec l'aide d'une carte à puce. Cette carte à puce et le sous-système décentralisé qui coopère avec elle sont librement accessibles par une personne éventuellement non autorisée.

Il est connu de chaîner divers moyens d'encryptage-décryptage dans un système de chiffrement-déchiffrement. Dans toute la suite, on appellera encryptage - décryptage un moyen de cryptage particulier utilisé dans un système plus vaste de chiffrement-déchiffrement.

On cherche depuis longtemps à optimiser le fonctionnement de ces systèmes du triple point de vue de la rapidité, de la place occupée en mémoire et de la sécurité. La rapidité s'entend au sens du temps nécessaire pour déchiffrer les données reçues.

Il est connu des systèmes d'encryptage - décryptage à clés symétriques. Leur sécurité inhérente peut être qualifiée en fonction de plusieurs critères.

Le premier critère est celui de la sécurité physique, relative à la facilité ou à la difficulté d'une méthode d'investigation par extraction de certains composants, suivie de leur remplacement éventuel par d'autres composants. Ces composants de remplacement, destinés à renseigner la personne non autorisée sur la nature et le fonctionnement du système de chiffrement-déchiffrement, sont choisis par elle de manière à ne pas être détectés, ou le moins possible, par le reste du système.

Pour améliorer la sécurité du système de chiffrement, il a été proposé des algorithmes à clé asymétriques, tels que les systèmes dits RSA (Rivest, Shamir et Adleman). Ces systèmes comprennent la génération d'une paire de clés appariées, l'une dite publique servant au chiffement, et l'autre dite privée servant au déchiffement. Ces algorithmes présentent un haut niveau de sécurité tant système que physique. Ils sont par contre plus lents que les systèmes traditionnels, surtout au stade du chiffement.

Les techniques d'attaque les plus récentes font appel à la notion dite DPA, de l'anglais Differential Power Analysis. Ces méthodes sont basées sur des supputations, vérifiables au bout d'un grand nombre d'essais, sur la présence d'un 0 ou d'un 1 dans une position donnée de la clé de chiffement. Elles sont quasiment non destructives, ce qui leur confère une bonne indétectabilité, et font appel à la fois à une composante d'intrusion physique et à une composante d'analyse mathématique. Leur fonctionnement rappelle les techniques d'investigation de champs pétrolifères, où une explosion de puissance connue est générée en surface et où des écouteurs et sondes, placés à des distances également connues du lieu de l'explosion, permettent d'émettre des suppositions sur la composition stratigraphique du sous-sol sans trop avoir à le creuser, grâce à la réflexion des ondes de choc par les limites de couches sédimentaires dans ce sous-sol. Les attaques DPA sont décrites notamment dans le § 2.1. du document "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", publié le 1er février 1999 par Suresh Chari, Charanjit Jutla, Josyula R. Rao et Pankaj Rohatgi, de l'IBM T.J. Watson Research Center, Yorktown Heights, NY.

L'exigence de devoir résister aux attaques DPA oblige à utiliser des systèmes de brouillage dit "whitening", soit dans les informations à l'entrée, soit en sortie d'un algorithme de chiffement-déchiffement. La technique du whitening est décrite dans le § 3.5 du même document précité.

De plus le fait que les puissances de calcul soient limitées dans le sous-système décentralisé d'un système de télévision à péage crée un problème, qui n'a jamais encore été résolu de façon satisfaisante, pour effectuer dans une mesure suffisante le chaînage décrit précédemment.

La chaînage peut démarrer dès que des données calculées en sortie du premier module sont partiellement disponibles pour être traitées par le second module.

- 5 L'invention permet de se prémunir contre les attaques précitées en combinant divers moyens d'encryptage-décryptage dans un système de chiffrement-déchiffrement, et en associant éventuellement une concaténation ou imbrication partielle à la séquence dans laquelle se suivent ces moyens.

10 Dans une forme particulière de réalisation de l'invention, le système de chiffrement-déchiffrement comprend un sous-système d'encodage où trois algorithmes sont utilisés séquentiellement:

- a) un algorithme A1 asymétrique à clé privée d1. Cet algorithme A1 effectue une signature sur des données en clair, représentées par un message m, cette opération délivrant un premier cryptogramme c1, au moyen d'opérations mathématiques généralement notées dans la profession par la
- 15 formule : $c1 = m \text{ exposant } d1, \text{ modulo } n1$. Dans cette formule, n1 fait partie de la clé publique de l'algorithme asymétrique A1, modulo représente l'opérateur mathématique bien connu des congruences dans l'ensemble des entiers relatifs, et d1 est la clé privée de l'algorithme A.

- b) un algorithme S symétrique utilisant une clé secrète K. Cet algorithme
- 20 convertit le cryptogramme c1 en un cryptogramme c2.

- c) un algorithme A2 asymétrique à clé privée d2. Cet algorithme A2 convertit le cryptogramme c2 en un cryptogramme c3, au moyen de l'opération mathématique notée, comme précédemment, par : $c3 = c2 \text{ exposant } d2 \text{ mod } n2$, formule dans laquelle n2 fait partie de la clé publique de
- 25 l'algorithme asymétrique A2, et d2 est la clé privée de l'algorithme A2

Le cryptogramme c3 part du sous-système d'encodage et parvient au sous-système décentralisé par des moyens connus en soi. Dans le cas de systèmes de télévision à péage, il peut s'agir aussi bien de données vidéo que de messages.

moyens de calcul nécessaires dans le sous-système décentralisé sont bien plus réduits que dans le sous-système d'encodage.

A titre d'exemple et pour fixer les idées, les étapes a) et c) c'est-à-dire les étapes d'encryptage avec clés privées, sont 20 fois plus longues que les
5 étapes d) et f) de décryptage avec clés publiques.

Dans une forme particulière de réalisation de l'invention, dérivée de la précédente, les algorithmes A1 et A2 sont identiques de même que leurs contreparties A1' et A2'.

Dans une forme particulière de réalisation de l'invention, également dérivée
10 de la précédente, dans l'étape c) on utilise la clé publique e2, n2 de l'algorithme asymétrique A2 alors que dans l'étape d) on décrypte le cryptogramme c3 avec la clé privée d2 de cet algorithme. Cette forme constitue une alternative possible lorsque les ressources du sous-système décentralisé en puissance de calcul sont loin d'être atteintes.

15 Bien que les cartes à puces sont utilisées majoritairement pour le décryptage des données, il existe également des cartes à puces ayant les capacités nécessaires pour effectuer des opérations de cryptage. Dans ce cas, les attaques décrites plus haut vont se porter également sur ces cartes de cryptage qui fonctionnent hors d'endroits protégés tels qu'un centre de
20 gestion. C'est pourquoi la méthode selon l'invention s'applique également aux opérations de cryptage en série c'est à dire que le module aval débute son opération de cryptage dès qu'une partie des informations délivrées par le module amont sont disponibles. Ce procédé à l'avantage d'imbriquer les différents modules de cryptage avec comme conséquence que le résultat du
25 module amont n'est pas disponible complètement à un temps donné. De plus, le module en aval ne débute pas ses opérations avec un résultat complet mais sur des parties ce qui rend impraticable d'interpréter le fonctionnement d'un module par rapport à un état d'entrée ou de sortie connu.

La présente invention sera comprise plus en détail grâce aux dessins
30 suivants, pris à titre non limitatifs, dans lesquels:

(voir figure 3) et lors du décryptage (voir figure 4), le module A2' utilise la clé privée d_2 , n_2 pour opérer. Bien que cette configuration présente une surcharge de travail à l'ensemble de décryptage, l'utilisation d'une clé privée renforce la sécurité offerte par le module A2.

- 5 L'exemple illustré aux figures 3 et 4 n'est pas restrictif pour d'autres combinaisons. Par exemple, il est possible de configurer le module A1 pour qu'il effectue l'opération d'encryptage avec la clé publique et le décryptage avec la clé privée.

- 10 Il est également possible de remplacer le module d'encryptage-décryptage à clé secrète S par un module de type à clé asymétriques du même type que les module A1 et A2.

8. Méthode selon la revendication 6, caractérisée en ce que les deux modules (A1, A2) utilisent un jeu différent de clés privée ($d1, n1$; $d2, n2$) et publique ($e1, n1$; $e2, n2$).

9. Méthode selon la revendication 5, caractérisée en ce que lors de l'encryptage, le dernier module (A2) utilise la clé dite publique ($e2, n2$) et lors du décryptage, le premier module (A2) utilise la clé dite privée ($d2, n2$).

10. Méthode selon les revendications 1 à 3, caractérisée en ce qu'elle met en œuvre trois modules (A1, A, A2) d'encryptage-décryptage à clés asymétriques.

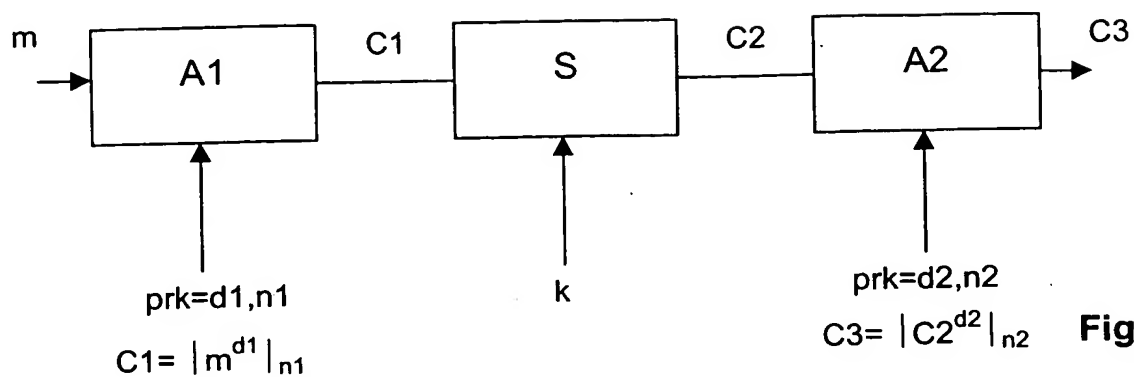


Fig. 1

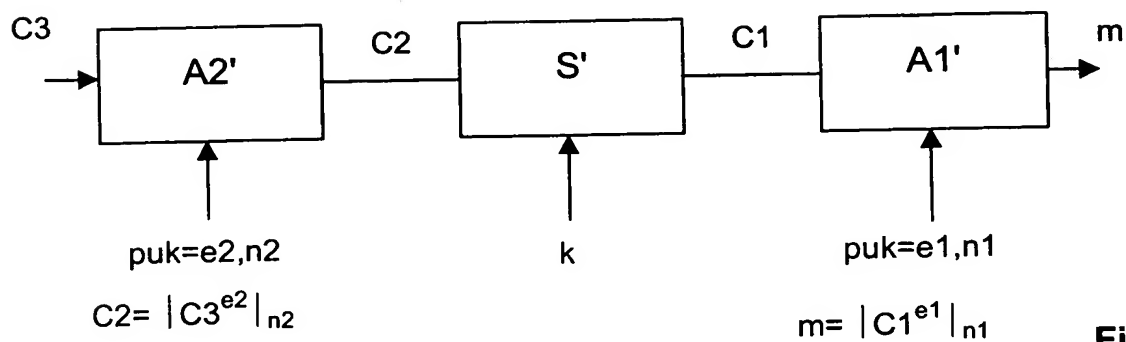


Fig. 2

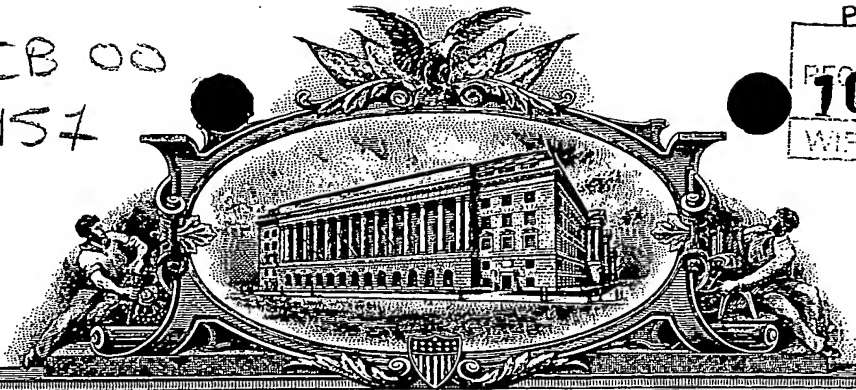
This Page Blank (uspto)

IB 00
01157

PA 279186

PCT / IB 00 / 01157
24.08.00

PCT
10/069714
WIPO PCT



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

July 24, 2000

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.


APPLICATION NUMBER: 60/194,171

FILING DATE: April 03, 2000

**DOCUMENT DE PRIORITÉ
PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)**



**By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS**


P. SWAIN
Certifying Officer

04/03/00
JC777 U.S. PTO

04-04-00

A/PROV

Please type a plus sign (+) inside this box → ☐

PTO/SB/16 (2-98)
Approved for use through 01/31/2001. OMB 0651-0037
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

JC541 U.S. PTO

60/194171

04/03/00

INVENTOR(S)					
Given Name (first and middle (if any))		Family Name or Surname		Residence (City and either State or Foreign Country)	
Christophe Marco Michael		Nicolas Sasselli John		Switzerland Switzerland Switzerland	
<input type="checkbox"/> Additional inventors are being named on the ___ separately numbered sheets attached hereto					
TITLE OF THE INVENTION (280 characters max)					
MULTI-MODULE ENCRYPTION METHOD					
Direct all correspondence to:			CORRESPONDENCE ADDRESS		
<input type="checkbox"/> Customer Number			Place Customer Number Bar Code Label here		
OR			Type Customer Number here		
<input checked="" type="checkbox"/> Firm or Individual Name			Clifford W. Browning		
Address			Woodard, Emhardt, Naughton, Moriarty & McNett		
Address			Bank One Center/Tower, 111 Monument Circle, Suite 370		
City			Indianapolis		
State			IN		
ZIP			46204-5137		
Country			USA		
Telephone			317-634-3456		
Fax			317-637-7561		
ENCLOSED APPLICATION PARTS (check all that apply)					
<input checked="" type="checkbox"/> Specification Number of Pages			13		
<input checked="" type="checkbox"/> Drawing(s) Number of Sheets			2		
<input type="checkbox"/> Small Entity Statement					
<input type="checkbox"/> Other (specify)					
METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)					
<input checked="" type="checkbox"/> A check or money order is enclosed to cover the filing fees			FILING FEE AMOUNT (\$)		
<input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number:			23-3030		
			\$150.00		
The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.					
<input checked="" type="checkbox"/> No.					
<input type="checkbox"/> Yes, the name of the U.S. Government agency and the Government contract number are: _____					

Respectfully submitted,

Date 04/03/00

SIGNATURE Clifford W. Browning

REGISTRATION NO. 32,201
(if appropriate)

TYPED or PRINTED NAME Clifford W. Browning

Docket Number: 16673-2

TELEPHONE 317-634-3456

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C., 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C., 20231.

MULTI-MODULE ENCRYPTION METHOD

5 The present invention relates to the domain of the encipherment, or encryption, and the decipherment or decryption of data, and particularly of data which is to remain inaccessible to unauthorized persons or appliances within the framework of pay-per-view television systems. In such systems, the data are enciphered in a secure environment, which accommodates
10 considerable computational power, and is called the encoding subsystem, and are then sent, by means known per se, to at least one decentralized subsystem where they are deciphered, generally by means of an IRD (Integrated Receiver Decoder) and with the aid of a
15 chip card. A possibly unauthorized person can gain unrestricted access to this chip card and the decentralized subsystem which cooperates with it.

20 It is known practice to chain together various encryption/decryption means in an enciphering/deciphering system. In all of what follows, the expression encryption/decryption will be used to refer to a particular encryption means used in a bigger enciphering/deciphering system.

25 It has long been sought to optimize the operation of these systems from the triple viewpoint of speed, memory space occupied and security. Speed is understood to mean the time required to decipher the data
30 received.

Encryption/decryption systems with symmetric keys are known. Their inherent security can be gauged as a function of several criteria.

35 The first criterion is that of physical security, relating to the ease or to the difficulty of a method of investigation by extracting certain components, this being followed by their possible replacement by other

00454471.010350

components. These replacement components, intended to inform the unauthorized person about the nature and manner of operation of the enciphering/deciphering system, are chosen by him/her in such a way as not to be detected, or to be as undetectable as possible, by the remainder of the system.

A second criterion is that of system security, within the framework of which attacks are not intrusive from the physical viewpoint but call upon analysis of mathematical type. Typically, these attacks will be conducted by computers of high power which will attempt to break the algorithms and the enciphering codes.

Means of encryption/decryption with symmetric keys are for example the systems referred to as DES (Data Encryption Standard). These relatively old means now merely offer system security and physical security which are entirely relative. It is for this reason in particular that increasingly, DES, the lengths of whose keys are too small to satisfy the conditions of system security, is being replaced by new means of encryption/decryption or with longer keys. Generally, these means having symmetric keys call upon algorithms comprising enciphering rounds.

Other attack strategies are referred to as Simple Power Analysis and Timing Analysis. In Simple Power Analysis, one uses the fact that a microprocessor tasked with encrypting or decrypting data is connected to a voltage source (in general 5 volts). When it is idle, a fixed current of magnitude i flows through it. When it is active, the instantaneous magnitude i is dependent, not only on the incoming data, but also on the encryption algorithm. Simple Power Analysis consists in measuring the current i as a function of time. The type of algorithm which the microprocessor is performing can be deduced from this.

SECRET 040300

In the same way, the method of Timing Analysis consists in measuring the duration of computation as a function of a sample presented to the decryption module. Thus, the relationship between the sample presented and the time for computing the result makes it possible to retrieve the decryption module secret parameters such as the key. Such a system is described for example in the document «Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems» published by Paul Kocher, Cryptography Research, 870 Market St, Suite 1088, San Francisco, CA-USA.

To improve the security of the enciphering system, algorithms having asymmetric keys have been proposed, such as the so-called RSA (Rivest, Shamir and Adleman) systems. These systems comprise the generation of a pair of matched keys, one the so-called public key serving in the enciphering, and the other the so-called private key serving in the deciphering. These algorithms exhibit a high level of security, both system and physical security. They are on the other hand slower than the traditional systems, especially at the enciphering stage.

The most recent attack techniques call upon the so-called DPA concept, standing for Differential Power Analysis. These methods are based on suppositions, verifiable after a large number of trials, about the presence of a 0 or a 1 in a given position of the enciphering key. They are almost non-destructive, thus rendering them largely undetectable, and call upon both a physical intrusion component and a mathematical analysis component. Their manner of operation recalls the techniques for investigating oil fields, where an explosion of known power is generated at the surface and where earphones and probes, placed at likewise known distances from the site of the explosion, enable assumptions to be made about the stratigraphic composition of the subsurface without having to carry

00154471, 040300

out too much digging, by virtue of the reflecting of the shock waves by the boundaries of sedimentary beds in this subsurface. DPA attacks are described in particular in § 2.1. of the document «A Cautionary Note
5 Regarding Evaluation of AES Candidates on Smart-Cards», published on 1st February 1999 by Suresh Chari, Charanjit Jutla, Josyula R. Rao and Pankaj Rohatgi, of IBM T. J. Watson Research Center, Yorktown Heights, NY.

10 The requirement of having to resist DPA attacks forces the use of so-called «whitening» jamming systems, either in the input information, or at the output of an enciphering/deciphering algorithm. The technique of whitening is described in § 3.5 of the same aforesaid
15 document.

Moreover, the fact that the computation powers are limited in the decentralized subsystem of a pay-per-view television system creates a problem, which has
20 never yet been satisfactorily solved, for performing the chaining described previously to a sufficient extent.

The objective of the present invention is to make
25 available an encryption/decryption method which is resistant to modern methods of investigation such as described above.

The objective aimed at by the present invention is
30 achieved by the method described in the characterizing part of Claim 1.

The particular feature of the method lies in the fact that an intermediate module does not start up when the
35 result from the previous (or upstream) module has terminated but begins as soon as already part of the information is available. Therefore, for an outside observer, it is not possible to establish the input or output conditions for this module.

60194471.040300

Since the deciphering occurs in the decentralized subsystem cooperating with the chip card, this chip card accommodating only relatively limited computational powers as compared with the encoding subsystem, it is for example beneficial to use a public asymmetric key, operating relatively fast, during the last steps of the deciphering. This makes it possible on the one hand to preserve the invulnerability characteristics of the system on exiting the procedure, and on the other hand to concentrate the computational power, related essentially to encipherment with the aid of the private key, in the encoding subsystem.

It has been discovered that extra security is afforded by the possibility of concatenating, or of partially interleaving, two means of encryption/decryption which follow one another sequentially. This concatenation or partial interleaving is understood to mean the process consisting in starting the action of the second encryption/decryption means on the data at a moment when the first encryption/decryption means has not yet terminated its work on these same data. This makes it possible to mask the data such as they would result from the work of the first module and before they are subjected to the action of the second module.

The chaining can start as soon as data computed at the output of the first module are partially available for processing by the second module.

The invention makes it possible to guard against the aforesaid attacks by combining various means of encryption/decryption in an enciphering/deciphering system, and possibly by associating concatenation or partial interleaving with the sequence in which these means follow one another.

6039471.040300

In a particular embodiment of the invention, the enciphering/deciphering system comprises an encoding subsystem where three algorithms are used sequentially:

5 a) an asymmetric algorithm A1 with private key d1. This algorithm A1 performs a signature on plain data, represented by a message m, this operation delivering a first cryptogram c1, by means of mathematical operations which are generally denoted in the
10 profession by the formula: $c1 = m \text{ exponent } d1, \text{ modulo } n1$. In this formula, n1 forms part of the public key of the asymmetric algorithm A1, modulo represents the well-known mathematical operator of congruences within the set of relative integers, and d1 is the private key
15 of the algorithm A.

b) a symmetric algorithm S using a secret key K. This algorithm converts the cryptogram c1 into a cryptogram c2.
20

c) an asymmetric algorithm A2 with private key d2. This algorithm A2 converts the cryptogram c2 into a cryptogram c3, by means of the mathematical operation denoted, as previously, by: $c3 = c2 \text{ exponent } d2 \text{ mod } n2$,
25 in which formula n2 forms part of the public key of the asymmetric algorithm A2, and d2 is the private key of the algorithm A2.

The cryptogram c3 leaves the encoding subsystem and
30 arrives at the decentralized subsystem by means known per se. In the case of pay-per-view television systems, this may equally involve video data or messages.

The decentralized subsystem uses, in the order reverse
35 to the above, three algorithms A1', S' and A2'. These three algorithms form part of three encryption/decryption means A1-A1', S-S' and A2-A2', distributed between the encoding subsystem and the

00154471.040300

decentralized subsystem, and representing the encryption/decryption system.

- 5 d) the algorithm $A2'$ performs a mathematical operation on $c3$ which restores $c2$ and is denoted: $c2 = c3 \text{ exponent } e2 \text{ mod } n2$. In this formula, the set consisting of $e2$ and $n2$ is the public key of the asymmetric algorithm $A2-A2'$.
- 10 e) the symmetric algorithm S' using the secret key K restores the cryptogram $c1$.
- 15 f) the asymmetric algorithm $A1'$ with public key $e1$, $n1$ retrieves m by performing the mathematical operation denoted: $m = c1 \text{ exponent } e1 \text{ mod } n1$.

The concatenation, in the decentralized subsystem, consists in starting the decoding step e) whilst $c2$ has not yet been completely restored by the previous step
20 d), and in starting the decoding step f) whilst $c1$ has not been completely restored by step e. The advantage is to thwart an attack aimed for example firstly at extracting, within the decentralized subsystem, the cryptogram $c1$ at the end of step e, so as to compare it
25 with the plaintext m , then by means of $c1$ and of m to attack the algorithm $A1'$, and then gradually to backtrack up the coding chain.

The concatenation is not necessary in the encoding
30 subsystem, which is installed in a secure physical environment. It is on the other hand useful in the decentralized subsystem. In the case of pay-per-view television, the IRD is in fact installed at the subscriber's premises and may be the subject of attacks
35 of the predescribed type.

It will be appreciated that an attack of a combination of three concatenated decryption algorithms $A1'$, S' and $A2'$ has much less chance of succeeding than if the

BO49471-040300

cryptograms c1 and c2 are fully reconstructed between each step d), e) and f). Moreover, the fact that the algorithms A1' and A2' are used with public keys e1, n1 and e2, n2 implies that the means of computation
5 required in the decentralized subsystem are much reduced as compared with those in the encoding subsystem.

By way of example and to fix matters, steps a) and c),
10 that is to say the encryption steps with private keys, are 20 times longer than the decryption steps d) and f) with public keys.

In a particular embodiment of the invention, derived
15 from the previous one, the algorithms A1 and A2 are identical as are their counterparts A1' and A2'.

In a particular embodiment of the invention, also derived from the previous one, in step c) the public
20 key e2, n2 of the asymmetric algorithm A2 is used whilst in step d) the cryptogram c3 is decrypted with the private key d2 of this algorithm. This embodiment constitutes a possible alternative when the resources of the decentralized subsystem in terms of
25 computational power are far from being attained.

Although chip cards are used chiefly for decrypting data, there are also chip cards having the capacities required to perform encryption operations. In this
30 case, the attacks described above will pertain also to these encryption cards which operate away from protected locations such as a management center. This is why the method according to the invention applies also to serial encryption operations, that is to say
35 that the downstream module begins its encryption operation as soon as part of the information delivered by the upstream module is available. This process has the advantage of interleaving the various encryption modules, and as a consequence the result from the

60494471.040300

upstream module is not completely available at a given time. Moreover, the downstream module does not begin its operations with a complete result but on parts, thereby making it impracticable to interpret the manner of operation of a module with respect to a known input state or output state.

The present invention will be understood in greater detail by virtue of the following drawings, taken by way of non-limiting example, in which:

- Figure 1 represents the encryption operations
- Figure 2 represents the decryption operations
- Figure 3 represents an alternative to the encryption method.

In Figure 1, a data set m is introduced into the encryption chain. A first element $A1$ performs an encryption operation using the so-called private key, composed of the exponent $d1$ and of the modulo $n1$. The result of this operation is represented by $C1$. According to the mode of operation of the invention, as soon as part of the result $C1$ is available, the next module begins its operation. This next module S performs its encryption operation with a secret key. As soon as it is partially available the result $C2$ is transmitted to the module $A2$ for the third encryption operation using the so-called private key composed of the exponent $d2$ and of the modulo $n2$. The final result, here dubbed $C3$, is ready to be transmitted by known pathways such as over the airwaves or by cable.

Figure 2 represents the decryption system composed of the three decryption modules $A1'$, S' , $A2'$ which are similar to those which served for encryption, but are ordered in reverse. Thus, one commences firstly with the module $A2'$ which performs its decryption operation on the basis of the so-called public key composed of the exponent $e2$ and of the modulo $n2$. In the same way

as for encryption, as soon as part of the result C2 from the module A2' is available, it is transmitted to the module S' for the second decryption operation. To terminate decryption, the module A1' performs its
5 operation on the basis of the so-called public key composed of the exponent e1 and of the modulo n1.

In a particular embodiment of the invention, the keys of the two modules A1 and A2 are identical, that is to
10 say that on the encryption side, $d1 = d2$ and $n1 = n2$. By analogy, during decryption, $e1 = e2$ and $n1 = n2$. In this case, one speaks of the private key d, n and of the public key e, n.

15 In another embodiment of the invention, as illustrated in Figures 3 and 4, the module A2 uses the so-called public key instead of the so-called private key. At the moment of encryption, the public key e2, n2 is used by the module A2, (see Figure 3) and during decryption
20 (see Figure 4), the module A2' uses the private key d2, n2 to operate. Although this configuration exhibits an overhead of work for the decryption set, the use of a private key reinforces the security offered by the module A2.

25 The example illustrated in Figures 3 and 4 is not restrictive in respect of other combinations. For example, it is possible to configure the module A1 so that it performs the encryption operation with the
30 public key and the decryption with the private key.

It is also possible to replace the encryption/ decryption module having secret key S with a module of the type with asymmetric keys of the same type as the
35 modules A1 and A2.

0045474.040300

CLAIMS

1. Method of encryption and decryption using several encryption/decryption modules in series, characterized in that the downstream encryption/decryption module begins its operation as soon as part of the result from the upstream encryption/decryption module is available.
2. Method according to Claim 1, characterized in that the downstream decryption module begins its decryption operation as soon as part of the result from the upstream decryption module is available.
3. Method according to Claim 1, characterized in that the downstream encryption module begins its encryption operation as soon as part of the result from the upstream module is available.
4. Method according to Claims 1 to 3, characterized in that it implements three modules (A1, S, A2), the central module (S) being of the type with secret symmetric key (k).
5. Method according to the preceding claim, characterized in that the first module (A1) and the last module (A2) in respect of encryption and the first module (A2) and the last module (A1) in respect of decryption are of the RSA type with asymmetric keys i.e. with a private key and a public key.
6. Method according to the preceding claim, characterized in that the two modules (A1, A2) use the so-called private key (d, n; d1, n1; d2, n2) for encryption and the so-called public key (e, n; e1, n1; e2, n2) for decryption.

60494171.040300

7. Method according to the preceding claim, characterized in that the two modules (A1, A2) use the same private key (d, n) and public key (e, n) set.
8. Method according to Claim 6, characterized in that the two modules (A1, A2) use a different set of private (d1, n1; d2, n2) and public (e1, n1; e2, n2) keys.
9. Method according to Claim 5, characterized in that during encryption, the last module (A2) uses the so-called public key (e2, n2) and during decryption, the first module (A2) uses the so-called private key (d2, n2).
10. Method according to Claims 1 to 3, characterized in that it implements three encryption/decryption modules (A1, A, A2) with asymmetric keys.

5049471.040300

- 13 -
ABSTRACT

When using an encryption/decryption module, there are methods in existence for determining the key or keys used by the module by analyzing the data entering or leaving the module. To alleviate this defect, the proposed multi-module method consists in the downstream module beginning its encryption/decryption operations as soon as part of the results from the upstream module is available.

60494471.040300

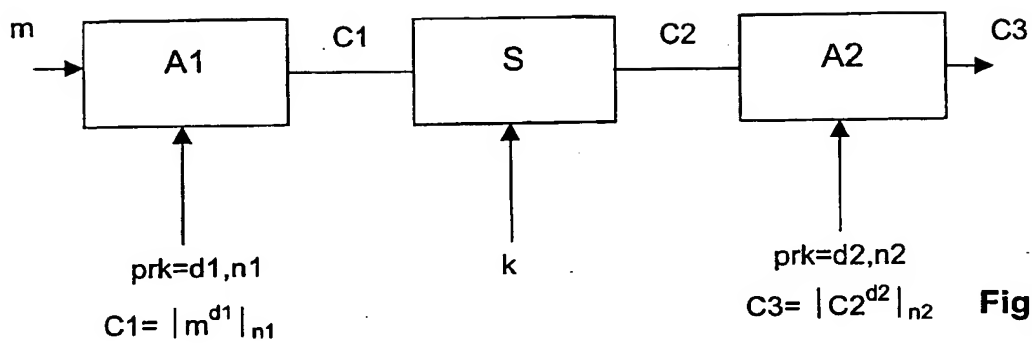


Fig. 1

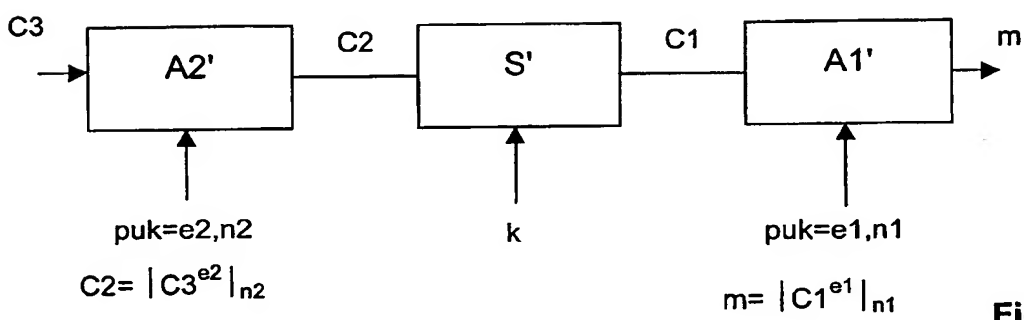


Fig. 2

005040.1746300



This Page Blank (uspto)